BP復号法に適した線形符号の設計 (符号と暗号の代数的数理)

AUTHOR(S):

渋谷, 智治

CITATION:

渋谷, 智治. BP復号法に適した線形符号の設計 (符号と暗号の代数的数理). 数理解析研究所講究録 2004, 1361: 80-90

ISSUE DATE:

2004-04

URL:

http://hdl.handle.net/2433/25261

数理解析研究所講究録 1361 巻 2004 年 80-90

BP復号法に適した線形符号の設計

渋谷 智治

Tomoharu Shibuya

文部科学省大学共同利用機関
メディア教育開発センター 研究開発部

R&D Department, National Institute of Multimedia Education

1 まえがき

誤り訂正符号とは, 情報を送信する側において送信情報に冗長を付加することによって, 通信路で生じた誤りを受信側において訂正することを可能にする符号化の技術である. 1990年代初頭に開発されたターボ符号 [2] や, その後再発見された low-density parity-check (LDPC) 符号 [6, 16] は誤り訂正符号の一クラスであり, 誤り訂正符号の性能限界 (シャノン限界 [3]) をほぼ達成する符号クラスであることから, 近年多くの研究者の注目を集めている. これらの符号が高い性能を示す鍵は, ビリーフ・プロパゲーション (BP) [18] の応用と今日では理解されている復号法 (BP 復号法) と, BP の近似精度が向上するような符号構成とにある.

より信頼性の高い通信を実現するためには, 実際に送信したビットと受信側で推定したビットとが異なる確率 (誤り率) を最小にするような復号戦略をとることが望ましい. このためには, 受信系列を条件とする送信符号語の条件付確率 (事後確率) を各送信ビットごとに周辺化する手続きが必要となるが, この手続きは一般に符号長の指数関数に比例する計算の手間を必要とする. このため実際の情報通信でこのような復号法が採用されることは殆ど無く, 上述した周辺化計算をより少ない手間で精度良く近似するための代替アルゴリズムがこれまでに数多く提案されてきた. その一つである BP 復号法は, 送信ビット間の依存関係に注意しながら局所的な計算を積み重ねることによって, 全体の周辺化の近似計算を効率よく行うアルゴリズムであり, 符号長に比例する計算の手間で周辺分布をきわめて精度良く近似することが可能である.

しかしながら, 符号語の各ビット間の依存関係を図式化した Tanner グラフ [22] と呼ばれる二部グラフに長さの短いループ, 特に長さ 4 のループが存在する場合, BP 復号法の近似精度が劣化することが知られている [16, 18]. Tanner グラフは符号の検査行列 [14] と一意に対応することから, 長さの短いループを含まない Tanner グラフを設計することにより, BP 復号に適した誤り訂正符号を設計することが可能である. 小文では, これまでに提案されてきた, 長さ 4 のループを含まない Tanner グラフの代表的な設計法を紹介する.

また, 巡回符号や代数幾何符号 [14] 等の従来の代数的な誤り訂正符号の検査行列は様々な代数的な構造を有することから, それらの符号の最小距離の評価は比較的容易であった. 一方, グラフに基づいて設計された誤り訂正符号の検査行列には, 最小距離の評価に従来用いられてきたような代数構造に乏しく, 最小距離の評価が非常に困難であった. これに対し, Tanner[23] は, Tanner グラフと密接に関連するグラフの隣接行列の固有値をグラフ理論的手法を用いて定式化することによって, グラフに基づいて設計された符号の最小距離の下界の導出に成功している. 小文では, この最小距離の下界を紹介する.

2 誤り訂正符号

本章では, 無記憶通信路上で生じた誤りを線形符号を用いて訂正する原理について説明する. なお, 情報通信における誤り訂正の一般的なモデル化については, 情報理論や符号理論の教科書 [3, 14, 19] を参照のこと.

2.1 線形符号

n を自然数とし, $\mathbb{F}_2 = \{0, 1\}$ を二つの要素からなる体とする. $\mathbb{F}_2^n$ の $\mathbb{F}_2$-線形部分空間 $C \subset \mathbb{F}_2^n$ を符号長 n の **2 元線形符号**または単に符号とよぶ.

$\mathbb{F}_2$-線形空間としての C の次元を k とおく. C の基底 $\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_k$ を行とする $k \times n$ 行列:

$$G := \begin{bmatrix} \boldsymbol{g}_1 \\ \boldsymbol{g}_2 \\ \vdots \\ \boldsymbol{g}_k \end{bmatrix}$$

を考えると, $C = \{\boldsymbol{i}G \mid \boldsymbol{i} \in \mathbb{F}_2^k\}$ が成り立つ. このことから, G を符号 C の**生成行列**という. 送信情報 $\boldsymbol{i} \in \mathbb{F}_2^k$ に生成行列 G を掛け合わせることを**符号化**といい, 得られた C の要素 $\boldsymbol{i}G$ を情報 $\boldsymbol{i}$ に対する**符号語**という.

$C^\perp$ を C に直交する $\mathbb{F}_2^n$ の元の集合:

$$C^\perp := \{\boldsymbol{v} \in \mathbb{F}_2^n \mid \boldsymbol{v} \cdot \boldsymbol{x} = 0 \text{ for all } \boldsymbol{x} \in C\}$$

とする. 但し, $\boldsymbol{v} \cdot \boldsymbol{x}$ は $\boldsymbol{v}$ と $\boldsymbol{x}$ の内積を表す. $C^\perp$ を生成する $\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_m \in \mathbb{F}_2^n$ に対して, それらを行とする $m \times n$ 行列

$$H := \begin{bmatrix} \boldsymbol{h}_1 \\ \boldsymbol{h}_2 \\ \vdots \\ \boldsymbol{h}_m \end{bmatrix}$$

を考えると, $\boldsymbol{x} \in \mathbb{F}_2^n$ が符号語であるための必要十分条件は $H\boldsymbol{x}^T = 0$ が成り立つこと, 即ち,

$$\boldsymbol{h}_i \cdot \boldsymbol{x} = 0, \quad i = 1, 2, \ldots, m \tag{1}$$

が成り立つことである．このことから，H を符号 C の**検査行列**という．また，k, m を符号 C の**情報点数**，**検査点数**という．一般に $m \geq n-k$ が成り立つ．

2.2 誤り訂正の原理

以下では C を符号とし，送信符号語および受信語をそれぞれ $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in C$，$\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in \mathcal{Y}^n$ で表す．但し $\mathcal{Y}$ は通信路の出力アルファベットを表す．また，$m \times n$ 行列 $H = (h_{ij})$ を C の検査行列とし，H に対して

$$A_i := \{j \mid h_{ij} = 1\}, \quad i = 1, 2, \ldots, m$$

と定める．

送信符号語は C から一様に選ばれるものとする．$\boldsymbol{x} \in \mathbb{F}_2^n$ が C の符号語であるための必要十分条件 (式 (1)) が，A_i を用いて $\sum_{j \in A_i} x_j = 0$ $(i = 1, 2, \ldots, m)$ と表せることに注意すると，$\boldsymbol{x} \in \mathbb{F}_2^n$ の事前分布 $p(\boldsymbol{x})$ は

$$p(\boldsymbol{x}) = \frac{1}{|C|} \prod_{i=1}^{m} \delta\Big(\sum_{j \in A_i} x_j, 0 \Big)$$

と表せる．但し

$$\delta(a, b) := \begin{cases} 1, & \text{if } a = b, \\ 0, & \text{if } a \neq b \end{cases}$$

である．

一方，通信路において誤りが生じる過程は，条件付確率 $p(\boldsymbol{y}|\boldsymbol{x})$ で表される．ここで，$p(\boldsymbol{y}|\boldsymbol{x}) = \prod_{j=1}^{n} p(y_j|x_j)$ が成り立つとき，通信路は**無記憶**であるという．以下では無記憶通信路上で通信が行われるものとする．

以上の仮定の下では，受信語 $\boldsymbol{y} \in \mathcal{Y}^n$ を得たときの，送信符号語 $\boldsymbol{x} \in C$ の事後分布 $p(\boldsymbol{x}|\boldsymbol{y})$ は，ベイズの公式より

$$p(\boldsymbol{x}|\boldsymbol{y}) = \frac{p(\boldsymbol{x})p(\boldsymbol{y}|\boldsymbol{x})}{\sum_{\boldsymbol{x}} p(\boldsymbol{x})p(\boldsymbol{y}|\boldsymbol{x})} = \kappa \prod_{i=1}^{m} \delta\Big(\sum_{j \in A_i} x_j, 0 \Big) \prod_{j=1}^{n} p(y_j|x_j) \tag{2}$$

と表される．但し κ は正規化定数であり，$\sum_{\boldsymbol{x} \in \mathbb{F}_2^n} p(\boldsymbol{x}|\boldsymbol{y}) = 1$ を満たすように定められる．

ここで，受信側で推定した符号語 $\hat{\boldsymbol{x}} \in C$ が送信符号語 $\boldsymbol{x}$ と異なる確率を最小にするためには，$\hat{\boldsymbol{x}} = (\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_n)$ を

$$\hat{\boldsymbol{x}} = \operatorname*{argmax}_{\boldsymbol{x} \in C} p(\boldsymbol{x}|\boldsymbol{y})$$

で定めればよい [19]．この復号は最大事後確率 (maximum a posteriori probability, MAP) 復号とよばれる[1]．一方，推定した各ビット $\hat{x}_j \in \mathbb{F}_2$ が送信ビット x_j と異なる確率を最小にするためには，$\hat{x}_j$ を

$$\hat{x}_j = \operatorname*{argmax}_{x_j \in \mathbb{F}_2} p(x_j|\boldsymbol{y})$$

[1] ここでは $\boldsymbol{x}$ の事前分布を一様と仮定しているので，最尤 (maximum likelihood, ML) 復号に一致する．

で定めればよい [19]. ここで, $p(x_j|\boldsymbol{y})$ は, $p(\boldsymbol{x}|\boldsymbol{y})$ の x_j に関する周辺分布

$$p(x_j|\boldsymbol{y}) := \sum_{x_1} \cdots \sum_{x_{j-1}} \sum_{x_{j+1}} \cdots \sum_{x_n} p(\boldsymbol{x}|\boldsymbol{y})$$

を表す. この復号は周辺事後確率 (maximizer of posterior marginals, MPM) 復号等とよばれることがある [11].

MAP 復号では, $p(\boldsymbol{x}|\boldsymbol{y})$ を最大にする符号語を C の全符号語 (2^k 個) から探索する必要がある. したがって, k が大きな場合には現実的な時間で MAP 復号を行うことは困難である. 一方 MPM 復号では, $p(\boldsymbol{x}|\boldsymbol{y})$ の周辺化に 2^{n-1} 個の $\boldsymbol{x} \in \mathbb{F}_2^n$ に対する $p(\boldsymbol{x}|\boldsymbol{y})$ の和を計算する必要があり, こちらも n が大きい場合に現実的な時間で復号を行うことは困難である.

このように, 誤り訂正における復号問題は計算量的に非常に困難な問題であるといえる. これに対し, BP [18] や sum-product アルゴリズム [5, 13] に基づく反復復号法 [6, 25] (以後, BP 復号法と呼ぶ) は, より少ない計算量で精度良く MPM 復号を近似する復号法である.

3 反復復号に適した二元線形符号

3.1 二元線形符号の Tanner グラフによる表現

互いに交わりの無いノードの集合 $V_c := \{c_i\}_{i=1}^m$, $V_v := \{v_j\}_{j=1}^n$ に対し, ノードの集合 V が $V := V_c \cup V_v$ で与えられ, 枝の集合 E が $E \subset V_c \times V_v$ を満たすような二部グラフ $\Gamma = (V, E)$ を考える. V_c, V_v のノードの次数がそれぞれ δ_c, δ_v で一定であるとき, Γ を特に (δ_v, δ_c)-正則二部グラフと呼ぶ.

Γ に対して, $\mathbb{F}_2$ 上の $m \times n$ 行列 $H_\Gamma := (h_{ij})$ を,

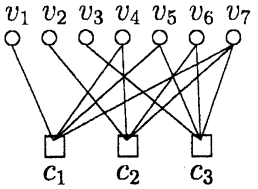
$$h_{ij} := \begin{cases} 1 \text{ if } (c_i, v_j) \in E, \\ 0 \text{ if } (c_i, v_j) \notin E \end{cases}$$

で定めると, H_Γ を検査行列とする, 符号長 n, 検査点数 m の二元線形符号

$$C_\Gamma := \{\boldsymbol{v} \in \mathbb{F}_2^n \mid H_\Gamma \boldsymbol{v}^T = \boldsymbol{0}\}$$

が定義できる. Γ を符号 C_Γ の **Tanner グラフ**[22] と呼ぶ. また, c_i, v_j はそれぞれ**検査ノード**, **変数ノード**と呼ばれる. 例として, 図 1 に $(7, 4, 3)$ Hamming 符号の検査行列 (図中 H) を与える Tanner グラフを示す.

BP 復号法の詳細についての説明は省略するが, Tanner グラフにループが存在しないとき, BP 復号法は MPM 復号法に一致することが知られている [16, 18]. しかしながら, ループを含まない Tanner グラフによって定義される符号は, 最小距離や符号化率等の符号自身の持つ誤り訂正能力が著しく劣る [4]. 一方, Tanner グラフがループを含むとき, 符号自身の誤り訂正能力は改善されるが, BP 復号法は MPM 復号法の近似となり, 復号性能の劣化を招くことが知られている [16]. さらに, 長さの短いループ, 特に長さ 4 のループが Tanner



$$H = \begin{pmatrix} 1001101 \\ 0101011 \\ 0010111 \end{pmatrix}$$

図 1: (7, 4, 3) Hamming符号の検査行列を与えるTannerグラフ.

グラフに多数含まれる場合には, その近似精度が著しく劣化する. そこで, 長さ4のループを含まないTannerグラフを構成する様々な手法が提案されている. 以下では, これまでに提案された代表的な手法を紹介する.

3.2 組み合わせデザインに基づくTannerグラフ

定義 1 [1,8] $\mathcal{P}$ を v 個の点の集合とする. $\mathcal{P}$ の k 個の異なる点の集合 B (ブロックと呼ぶ) の族 $\mathcal{B}$ について, $\mathcal{P}$ の t 個の点からなる任意の集合が $\mathcal{B}$ の λ 個のブロックに含まれるとき, $\mathcal{P}$, $\mathcal{B}$ を t-(v, k, λ) デザインと呼ぶ. □

t-(v, k, λ) デザインが与えられたとき, ノードの集合を $V_c = \mathcal{B}$, $V_v = \mathcal{P}$ とおき, さらに枝の集合を

$$E := \{(B, p) \in \mathcal{B} \times \mathcal{P} \mid p \in B\}.$$

で定めることによって, 平行枝の無い二部グラフ $\Gamma_t(v, k, \lambda) = (V_v \cup V_c, E)$ が得られる.

命題 2 [1] $\Gamma_t(v, k, \lambda)$ は変数ノード数 v, 検査ノード数 $v\delta_v/k$ の (δ_v, δ_c)-正則二部グラフとなる. 但し,

$$\delta_v = \frac{\lambda \binom{v-1}{t-1}}{\binom{k-1}{t-1}}, \quad \delta_c = k$$

である. □

命題2より, t-(v, k, λ) デザインの点及びブロックはTannerグラフにおける変数ノードおよび検査ノードとみなすことができる.

t-$(v, k, 1)$ $(t \geq 2)$ はSteinerシステムと呼ばれる [1,8]. 特に $t = 2$ のとき, 以下の命題が成り立つ.

命題 3 [10] $\Gamma_2(v, k, 1)$ は長さ4のループを含まない. □

このことから, $\Gamma_2(v, k, 1)$ をTannerグラフとする符号の性能については, 比較的早い段階から検討がなされてきた [17]. 以後, $\Gamma(v, k) := \Gamma_2(v, k, 1)$ とする.

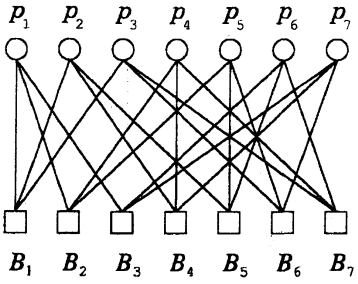


図 2: $\Gamma(7,3)$: 2-$(7,3,1)$ デザインから得られる二部グラフ.

例 4 $\mathcal{P} := \{p_1, p_2, \ldots, p_7\}$ とし,

$$\mathcal{B} := \{B_1, B_2, \ldots, B_7\}$$
$$= \{\{p_1,p_2,p_3\},\{p_1,p_4,p_5\},\{p_1,p_6,p_7\},\{p_2,p_4,p_7\},\{p_2,p_5,p_6\},\{p_3,p_5,p_7\},\{p_3,p_4,p_6\}\}.$$

とおく. このとき, $\mathcal{P}$, $\mathcal{B}$ は 2-$(7,3,1)$ デザインとなり, 二部グラフ $\Gamma(7,3)$ が構成できる. 図 2 に $\Gamma(7,3)$ を示す. 図中の丸および四角は, それぞれ点およびブロックに対応する. 図 2 に示すように, $\Gamma(7,3)$ は $(3,3)$-正則二部グラフとなる. □

3.3 $\Gamma(v,k)$ の変形によって得られる Tanner グラフ

$\Gamma(v,k)$ から

- ある変数ノード b, および
- b に隣接している全ての検査ノード

を取り除き, 更に取り除かれたノードに接続していた全ての枝を取り除いたグラフを $\Gamma'(v,k)$ で表す. 例として, 図 3 に $\Gamma(7,3)$ から $\Gamma'(7,3)$ を得る様子を示す. $\Gamma(7,3)$ における黒く塗りつぶされたノードおよび破線は, 取り除かれるノードと枝を表す.

命題 3 より $\Gamma(v,k)$ には長さ 4 のループが含まれないことから, $\Gamma'(v,k)$ にも長さ 4 のループは含まれない. また, $\Gamma'(v,k)$ を考えることによって, 符号パラメータや復号性能が改善できることが報告されている [9, 10].

3.4 EG-LDPC 符号

2^s 個の元からなる体 $\mathbb{F}_{2^s}$ 上の m 次元ユークリッド幾何 (Euclidean geometry) [1] を $\mathrm{EG}(m,2^s)$ で表す. $\mathrm{EG}(m,2^s)$ は 2^{ms} 個の点と $2^{(m-1)s}(2^{ms}-1)/(2^s-1)$ 本の直線とからなり, 各直線上には 2^s 個の点が存在し, 任意の二直線は一点で交わる. $\mathrm{EG}(m,2^s)$ の点と直線を t-デザインにおける点とブロックに対応させることにより, $\mathrm{EG}(m,2^s)$ は $t=2$, $v=2^{ms}$, $k=2^s$ の Steiner システムとみなせる [1].

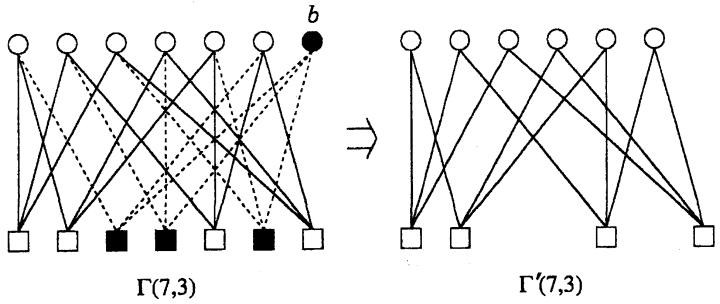


図 3: $\Gamma(7,3)$ から $\Gamma'(7,3)$ を得る際に取り除かれるノードおよび枝.

b を $\Gamma(2^{ms},2^s)$ の変数ノードのうち $\mathrm{EG}(m,2^s)$ の原点に対応する点とし, 前節の手法によって b と b に関連するノード及び枝を取り除いた二部グラフ $\Gamma' := \Gamma'(2^{ms},2^s)$ を考える. このとき, Kou ら [12] によって提案されたタイプ I EG-LDPC 符号は $C_{\Gamma'}$ と表されることが容易に示される. 従って, $\Gamma'(2^{mx},2^s)$ で与えられるタイプ I EG-LDPC 符号の Tanner グラフには長さ 4 のループは存在しない.

3.5 Cayley グラフに基づく Tanner グラフ

定義 5 [7] G を有限群とし, $A \subset G$ を, 任意の $a \in A$ に対して $a^{-1} \in A$ が成り立つ部分集合とする. G の元をノードの集合とし, $\{(g,h) \in G \times G \mid hg^{-1} \in A\}$ を枝の集合とするグラフ $\Gamma(G,A)$ を Cayley グラフという. □

命題 6 [15] q を奇素数とする. $G := SL_2(\mathbb{F}_q)$ とし, $A \subset G$ を

$$A := \left\{ a = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, a^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, b^{-1} = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \right\}$$

とおくと, $\Gamma(G,A)$ はノード数 q^3-q で, 各ノードの次数が 4 である正則グラフとなる. また, グラフの内径は $2\log_s(q/2)-1$ $(s=1+\sqrt{2})$ 以上となる. □

Margulis は, 命題 6 で与えられた Cayley グラフ $\Gamma(G,A)$ から, 以下の手順により二部グラフを構成した.

まず, 二部グラフの一方のノードとして, G のコピー $G, \tilde{G}$ を割り当てる. 次に, 他方のノードして G のコピー $\hat{G}$ を割り当てる. 枝の割り当ては

- $g \in G$ を $ga^2, gaba^{-1}, gb \in \hat{G}$ と接続する
- $\tilde{g} \in \tilde{G}$ を $\tilde{g}a^{-2}, \tilde{g}ab^{-1}a^{-1}, \tilde{g}b^{-1} \in \hat{G}$ と接続する

ことによって行う. このようにして, 変数ノード数 $2(q^3-q)$, 検査ノード数 q^3-q の $(3,6)$-正則二部グラフが得られる.

A の元を掛け合わせて G の単位元を生成するときに必要な A の元の最小個数を c とする. 但し, その積の中には $aa^{-1}, a^{-1}a, bb^{-1}, b^{-1}b$ といった, 単位元を与える自明な関係が含まれていないものとする. このとき,

$$\{a^2, a^{-2}, aba^{-1}, ab^{-1}a^{-1}, b, b^{-1}\}$$

の元を掛け合わせて単位元を生成するために必要な要素の個数は (自明な関係を除いて) $c/2-1$ 以上である. このことから, 上記の方法で得られた二部グラフの内径は $\log_s(q/2)-1$ $(s=1+\sqrt{2})$ 以上であることが分かる. q が十分に大きなとき, 得られた二部グラフは長さ 4 のループを持たない.

このほかにも, 内径の大きなCayleyグラフから二部グラフを構成する手法がいくつか提案されている [20, 24].

4 隣接行列の固有値に基づく最小距離の下界

Γ が (δ_v, δ_c)-正則なTannerグラフの場合, Γ に密接に関連するあるグラフの接続行列の固有値を用いて, C_Γ の最小距離 $d(C_\Gamma)$ の下界を与えることができる.

H_Γ を 0, 1 からなる実行列とみなし, $H_\Gamma^T H_\Gamma$ の相異なる固有値を $\mu_1, \mu_2, \ldots, \mu_s$ $(\mu_i > \mu_{i+1})$ で表す.

命題 7 [23] 変数ノード数 n のTannerグラフ Γ が連結で, 変数ノード, 検査ノードの次数がそれぞれ一様に δ_v, δ_c ならば, $d(C_\Gamma) \geq \max\{d_1, d_2\}$ が成り立つ. 但し,

$$d_1 := \frac{n(2\delta_v - \mu_2)}{\delta_v\delta_c - \mu_2}, \quad d_2 := \frac{2n\{2(\delta_v - 1) + \delta_c - \mu_2\}}{\delta_c(\delta_v\delta_c - \mu_2)}$$

である. □

与えられた Γ に対して命題7の下界を計算するためには, $H_\Gamma^T H_\Gamma$ の二番目に大きな固有値 μ_2 を実際に求めればよい. さらに, ある種のクラスのTannerグラフについては, 以下に述べるグラフ理論的手法によって μ_2 を定式化することができる.

平行な枝や始点と終点の一致する枝の無いグラフ $\Pi = (W, F)$ について, $|W| = v$ かつ Π の全ノードの次数が α であり, さらに $w_i, w_j \in W$ について $S_{ij} := \{w_k \in W \mid (w_i, w_k), (w_j, w_k) \in F\}$ と定義したとき

$$|S_{ij}| = \begin{cases} \beta, (w_i, w_j) \in F, \\ \gamma, (w_i, w_j) \notin F \end{cases}$$

が成り立つとき, Π はパラメタ $(v, \alpha, \beta, \gamma)$ の**強正則グラフ** [7] であるという. また, グラフ $\Pi = (W, F)$ $(W = \{w_1, w_2, \ldots, w_n\})$ の**隣接行列** $A_\Pi = (a_{ij})$ とは,

$$a_{ij} := \begin{cases} 1 \text{ if } (w_i, w_j) \in F, \\ 0 \text{ if } (w_i, w_j) \notin F \end{cases}$$

で定義される $n \times n$ 行列である. このとき次の命題が知られている.

命題 8 [7] パラメタ (v,α,β,γ) の強正則グラフの隣接行列は, 異なる 3 つの固有値:

$$\alpha, \quad \frac{1}{2}\left\{\beta-\gamma \pm \sqrt{(\beta-\gamma)^2+4(\alpha-\gamma)}\right\}$$

を有する. さらに, これらの固有値の重複度は

$$1, \quad \frac{1}{2}\left\{v-1 \pm \frac{(v-1)(\gamma-\beta)-2\alpha}{\sqrt{(\beta-\gamma)^2+4(\alpha-\gamma)}}\right\}$$

である. □

$\Gamma=(V_v \cup V_c, E)$ に対して, Γ の**ポイントグラフ** [7] $\Pi_\Gamma := (W,F)$ を $W=V_v$,

$$F := \{(v_i,v_j) \in V_v \times V_v \mid i \neq j, (c,v_i),(c,v_j) \in E \text{ for some } c \in V_c\}$$

で定義する. 3 章で取り上げた Steiner システムに基づく Tanner グラフやタイプ I EG-LDPC 符号の Tanner グラフについては, それらのポイントグラフ Π_Γ が強正則グラフであり, そのパラメタが定式化できる [9,21]. さらに

$$A_{\Pi_\Gamma} = H_\Gamma^T H_\Gamma - \delta_v I$$

の関係が成り立つことが知られている [9,21]. 従って, 命題 8 によって求められる A_{Π_Γ} の二番目に大きな固有値を ν_2 とおくと, $\mu_2=\nu_2+\delta_v$ により μ_2 が求められる.

5 むすび

本稿では, BP 復号法に適した線形符号を Tanner グラフに基づいて設計するために, これまでに提案されてきた長さ 4 のループを含まない二部グラフの構成方法を紹介した. また, これらの符号の最小距離を Tanner グラフに基づいて解析する手法を紹介した. 今後の研究では, より性能の良い LDPC 符号の設計にこれらの手法が役立てられることが期待される.

参考文献

[1] E. F. Assmus, Jr. and J. D. Key, *Designs and Their Codes*, Cambridge University Press, 1992.

[2] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," *Proc. of ICC* (Geneva), pp.1064–1070, 1993.

[3] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley Series in Telecommunications, Wiley, 1991.

[4] T. Etzion, A. Trachtenbeg, and A. Vardy, "Which codes have cycle-free Tanner graphs?", *IEEE Trans. Inform. Theory*, vol.IT-45, pp.2173–2181, 1999.

[5] B. J. Frey, *Graphical Models for Machine Learning and Digital Communication*, The MIT Press, 1998.

[6] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory* vol.IT-8, pp.21–28, 1962.

[7] C. Godsil and G. Royle, *Algebraic Graph Theory*, GTM 207, Springer-Verlag, New York, 2001.

[8] M. Hall, Jr., *Combinatorial Theory*, 2nd ed., Wiley, New York, 1983.

[9] S. J. Johnson and S. R. Weller, "Construction of low-density parity-check codes from Kirkman triple systems," *Proceedings of IEEE Globecom'01* (San Antonio, USA), vol.2, pp.970–974, 2001.

[10] S. J. Johnson and S. R. Weller, "Codes for iterative decoding from partial geometries," *Proceedings of IEEE ISIT 2002* (Lausanne, Switzerland), p.310, 2002. available from http://www.ee.newcastle.edu.au/users/staff/steve.

[11] 汪 金芳, 田栗 正章, 手塚 集, 樺島 祥介, 上田 修功, 計算統計 I, 確率計算の新しい手法 (統計科学のフロンティア 11), 岩波書店, 2003.

[12] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries : A rediscovery and new results," *IEEE Trans. Inform. Theory*, vol.IT-47, pp.2711–2736, 2001.

[13] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inform. Theory*, vol.47, pp.498–519, 2001.

[14] J. H. van Lint, *Introduction to Coding Theory*. Springer-Verlag, second ed., 1991.

[15] G. A. Margulis, Explicit constructions of graphs without short cycles and low density codes. *Combinatorica*, vol.2, no.1, pp.71–78, 1988.

[16] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol.IT-45, pp.399–431, 1999.

[17] D. J. C. MacKay and M. C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," *Codes, Systems, and Graphical Models* (B. Marcus and J. Rosenthal, Eds.), The IMA Volumes in Mathematics and its Applications, vol.123, Springer-Verlag, New York, pp.113–130, 2001.

[18] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann Publishers, 1988.

[19] J. G. Proakis, *Digital Communications*, 3rd. ed., McGraw-Hill, 1995.

[20] J. Rosenthal and P. O. Vontobel, "Constructions of LDPC Codes using Ramanujan Graphs and Ideas from Margulis," *Proc. of 38th Allerton Conf. on Communication, Control, and Commuting*, pp.248–257, 2000.

[21] T. Shibuya, M. Onikubo, and K. Sakaniwa, "On Tanner's lower bound for the minimum distance of regular LDPC codes based on combinatorial designs," *IEICE Trans. Fundamentals*, vol.E86-A, no.10, pp.2428–2435, 2003.

[22] R. M. Tanner, "A Recursive Approach to Low Complexity Codes," *IEEE Trans. Inform. Theory*, vol.27, pp.533–547, Sep. 1981.

[23] R. M. Tanner, "Minimum-Distance Bounds by Graph Analysis," *IEEE Trans. Inform. Theory*, vol.47, pp.808–821, Feb. 2001.

[24] J.-P. Tillich and G. Zémore, "Optimal Cycle Codes Constructed from Ramanujan Graphs," *SIAM J. Discrete Math.*, vol.10, no.3, pp447–459, 1997.

[25] T. Wadayama, *Low-density parity-check codes and their decoding algorithms*, Triceps, 2002.